厚生労働省情報セキュリティ報告書

2012 年 5 月 25 日

厚生労働省情報セキュリティ委員会

＜ 目　次 ＞

はじめに　～最高情報セキュリティ責任者のメッセージ～　.....3

１　厚生労働省における情報セキュリティ対策の枠組み　.....4

２　平成 23 年度における情報セキュリティ対策の取組　.....8

３　情報セキュリティ対策に関する平成 24 年度の計画　.....24

終わりに　～最高情報セキュリティアドバイザーからのメッセージ～　.....25

はじめに　～最高情報セキュリティ責任者のメッセージ～

近年の情報通信技術の急速な進歩により、ＩＴ（情報技術）の活用は、行政事務の遂行に当たって、なくてはならないものになっています。その一方で、インターネットの脆弱性を狙った攻撃ツールや新種のウィルスを利用した攻撃等は日々発生しており、不正アクセスや情報漏えい等のリスク・脅威は拡大している状況です。

このような情勢の中、厚生労働省は、医療や年金、雇用対策など、国民生活に直結する政策を担っていることから、業務で取り扱う情報資産は、適切な運用管理の下、あらゆる脅威から守らなくてはなりません。そのためには、必要な情報セキュリティの確保とその継続的な強化・拡充に取り組むことが不可欠です。

本報告書は、平成23年度に厚生労働省が取り組んだ情報セキュリティ対策の実施状況等についてまとめたものです。厚生労働省では、これまでも、

(1)情報セキュリティ教育の実施
(2)情報セキュリティ監査の実施
(3)情報セキュリティ対策の普及・啓発及び注意喚起
(4)情報セキュリティ対策実施状況の自己点検及び重点検査の実施

を中心に、情報セキュリティ対策を実施してきたところです。平成23年度は、防衛産業へのサイバー攻撃、また、衆議院や政府機関もサイバー攻撃を受けていたことが明らかになるなど重大事案が頻発したことを受け、セキュリティ事案の発生時など、様々な機会をとらえ、セキュリティ対策の注意喚起や厚生労働省情報セキュリティポリシーの周知・徹底に努めたところです。

平成23年度全体を通してみると、平成22年度とほぼ同様の実施結果であったことから、来年は全体的に底上げされるよう、各対策について改善努力を行う必要があります。

厚生労働省としましては、今後も情報セキュリティを取り巻く環境や情報通信技術の動向を踏まえつつ、新たなリスク・脅威にも適切に対応するとともに、平成23年度の実施内容を一層充実させるなど、引き続き、情報セキュリティ対策の維持・強化に努めてまいります。

最高情報セキュリティ責任者
（厚生労働省大臣官房長）
岡崎　淳一

1　情報セキュリティ対策の枠組み

この章では、厚生労働省の基本的な情報と推進体制等の情報セキュリティ対策の枠組みについて報告する。

（1）厚生労働省の基本的な情報

①　厚生労働省の概要

厚生労働省は、人の誕生から雇用、子育て、医療、老後の保障まで、国民生活を支える重要かつ広範な分野を担う省であり、これらに関する様々な行政事務を着実かつ円滑に進めるために必要な情報システムを構築・運用している。

②　対象とする期間

本報告書が対象とする期間は、平成 23 年 4 月 1 日から平成 24 年 3 月 31 日までの１年間とする。

③　対象とする組織

本報告書が対象とする組織は、厚生労働省の本省、地方支分部局、施設等機関及び中央労働委員会事務局とする。

④　対象とする情報

本報告書が対象とする情報は、「政府機関の情報セキュリティ対策のための統一管理基準」及び「厚生労働省情報セキュリティポリシー」（以下「セキュリティポリシー」という。）の定義に基づき、以下のとおりとする。

○　情報システム内部に記録された情報
○　情報システム外部の電磁的記録媒体に記録された情報
○　情報システムに関係がある書面に記録された情報

⑤　報告書作成部署

大臣官房統計情報部情報システム課

（2）情報セキュリティ対策に関する文書体系

①　基本方針及び対策基準

厚生労働省では、情報セキュリティ対策の基本方針及び省庁対策基準として、「政府機関の情報セキュリティ対策のための統一規範」、「政府機関の情報セキュリティ対策のための統一管理基準」、「政府機関の情報セキュリティ対策のための

統一技術基準」（以下あわせて「統一基準群」という。）に準拠したセキュリティポリシーを策定している。また、これを遵守するための具体的な手順書として、以下の関連規程類を整備している。

○　情報取扱手順書
○　例外措置手順書
○　情報セキュリティ対策実施手順書作成のガイドライン
○　障害・事故等対処手順書
○　人事異動等の際に行うべき情報セキュリティ対策実施規程
○　厚生労働省支給以外の情報システムによる情報処理の手順書
○　省外でのＰＣの利用における情報処理の手順書
○　省外の情報セキュリティ水準の低下を招く行為の防止に関する規程
○　外部委託における情報セキュリティ対策実施手順書

②　文書の見直し状況

統一基準群が改訂された際や情報セキュリティ監査における指摘があった際等において、情報セキュリティを取り巻く状況も加味しながら、適宜、セキュリティポリシー及び関連規程類を見直し、必要な改訂を行うとともに、職員への周知を確実に行い、適切な情報セキュリティ対策が確保されるようにしている。

③　情報資産台帳の整備と活用

情報システムごとに基本情報（システムの概要、管理部局及び責任者名等）、セキュリティ対策の実施状況、ハードウェア・ソフトウェアに関する情報、取り扱う情報の種類等を記載した情報資産台帳を整備している。これにより、保有する情報システムを網羅的に把握し、更なる最適化の拡大・推進を図るとともに、各情報システムのセキュリティ水準の把握、脆弱性に対するフォローアップ等に活用している。

④　業務継続計画の策定

厚生労働省の業務は、医療や年金、雇用対策等、国民生活に直結しており、首都直下地震等の不測の事態の発生時においても、その断絶は国民生活等に重大な影響を及ぼすおそれがある。

このような状況や平成 23 年 3 月に発生した東日本大震災の教訓も踏まえ、別途策定している業務継続計画において継続することが重要とされる業務に必要な情報システムを中心に、情報システムの運用継続に特化した業務継続計画（情報システム運用継続計画）の策定を進め、不測の事態の発生に備えている。

（3）情報セキュリティ対策の推進体制

厚生労働省では、情報セキュリティ対策を推進するため図１に示す推進体制を整備し、それぞれの権限と責務に応じた情報セキュリティ対策に取り組んでいる。

① 責任者等の主な役割

○ 最高情報セキュリティ責任者

厚生労働省におけるセキュリティ対策に関する事務を統括する。

○ 情報セキュリティ委員会

セキュリティポリシーの策定等を行うための組織。各部局の筆頭課長等で構成され、最高情報セキュリティ責任者が委員長として議事を統括する。

○ 情報セキュリティ監査責任者

情報セキュリティ監査に関する事務を統括する。

○ 統括情報セキュリティ責任者

情報セキュリティ責任者を統括し、省統一で整備する実施手順書・各種計画等の策定を行う。

○ 統括情報セキュリティ管理者

統括情報セキュリティ責任者を補佐する。

○ 情報セキュリティ責任者

所管する部局等の情報セキュリティ対策に関する事務を統括する。

○ 部局情報セキュリティ管理者

情報セキュリティ責任者を補佐する。

○ 課室情報セキュリティ責任者

課室等の情報セキュリティ対策に関する事務を統括する。

○ 課室情報セキュリティ管理者

課室情報セキュリティ責任者を補佐する。

○ 情報システムセキュリティ責任者

所掌する情報システムの情報セキュリティ対策に関する事務を統括する。

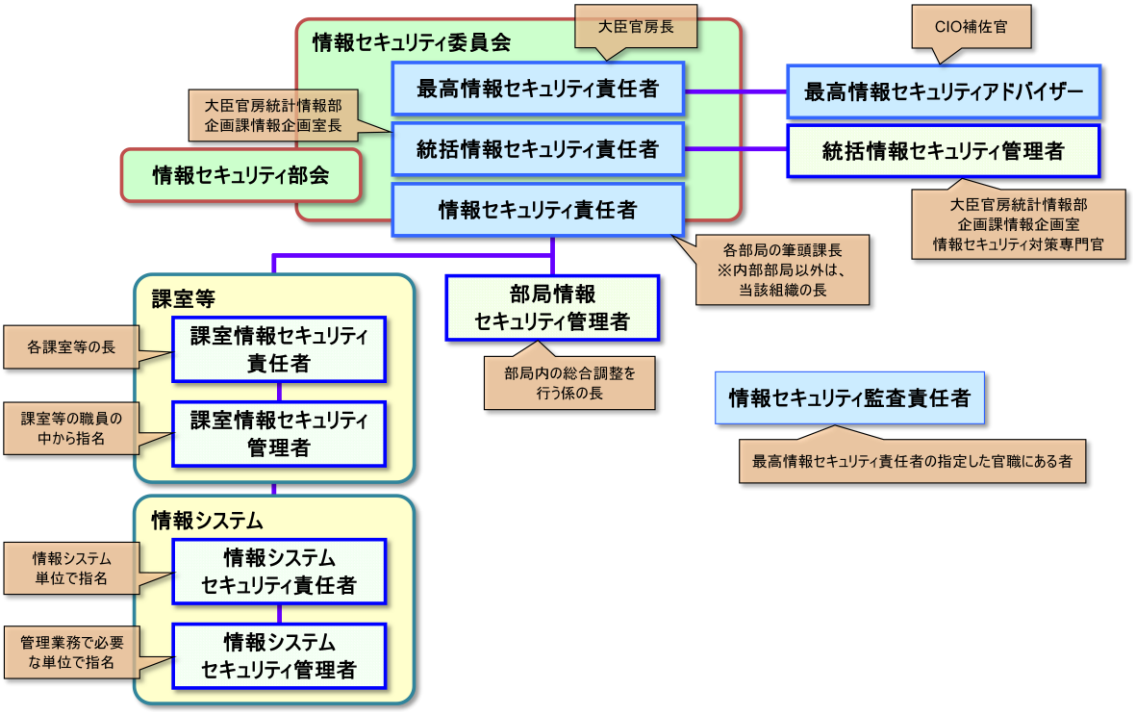
○　情報システムセキュリティ管理者

所掌する情報システムの管理業務において必要な単位ごとに置かれ、情報システムに係る情報セキュリティ対策を実施する。

○　最高情報セキュリティアドバイザー

最高情報セキュリティ責任者を補佐し、省全体の情報セキュリティ対策全般に対して助言等を行う。

図１　情報セキュリティ対策の推進体制



②　統一基準群とセキュリティポリシーの相違点

セキュリティポリシーにおいては、統一基準群に規定されていない「統括情報セキュリティ管理者」、「部局情報セキュリティ管理者」、「課室情報セキュリティ管理者」を、それぞれ統括情報セキュリティ責任者、情報セキュリティ責任者、課室情報セキュリティ責任者の業務を補佐する者として、各責任者が指名することとしている。管理者が責任者を補佐することで、障害・事故等の緊急時を始め、必要な対応の迅速化・効率化を図っている。

2　平成23年度における情報セキュリティ対策の取組

厚生労働省における情報セキュリティ対策の取組は、セキュリティポリシーに基づき実施されている。内閣官房情報セキュリティセンター（National Information Security Center。以下「NISC」という。）を始め、関係機関とも連携をとっている。

この章では、平成23年度における厚生労働省の取組について報告する。

（1）平成23年度における重点事項

①　情報管理対策の強化

平成22年度に発生した尖閣諸島沖中国漁船衝突映像の流出事件以来、これまで以上に政府機関における情報管理の徹底が厳しく求められている。

このような状況を踏まえ、セキュリティポリシー及び関連規程類の一部を改訂し、クラウド技術への対応を意識した情報の保存に係る対策、外部からの不正アクセスに係る対応、情報漏えい対策、障害・事故等対応の更なる強化を図った。

また、各種研修における教育の場や、毎年度１０月の電子政府利用促進週間、同２月の情報セキュリティ月間、障害・事故等の発生時といった情報セキュリティに関連するイベント等の機会をとらえ、情報管理の重要性について周知・徹底を図った。

②　送信ドメイン認証技術導入の推進

近年、メールを介して特定の組織（企業・政府機関等）を狙った情報セキュリティ上の攻撃（ウイルス感染、スパイウェアによる情報搾取等）を仕掛ける標的型メール攻撃が社会的な問題となっている。標的型メールは、送信者を詐称して送付される場合が多く、政府機関の職員を騙って送付される場合も見受けられる。

このため、厚生労働省から送信されるメールが、確実に厚生労働省から送付されたものであることを保証するための技術として、送信ドメイン認証（Sender Policy Framework）技術の導入が喫緊の課題であったが、これに係る取組の結果、本報告書が対象とする組織で所有する go.jp ドメイン（○○○.go.jp）については、すべて対策が完了した。

（2）情報セキュリティ教育

①　教育計画

情報セキュリティ対策を適切に実践するためには、職員一人一人がセキュリティポリシー及び関連規程類を理解し、遵守することが必要である。

このため、「情報セキュリティ対策教育計画」を年度ごとに策定し、これに従って職員が情報セキュリティ対策に関する教育を受講することにより、適切な対策

が実践されるようにしている。

② 研修

各種教育教材については、セキュリティポリシー及び関連規程類の改訂や最新の情報セキュリティ事案の発生状況、更には前年度の各種点検・調査結果や研修受講後のアンケート結果等も踏まえ、適宜、見直しを行っており、平成23年度においても、平成23年度の重点事項に関する内容や情報システム運用継続計画、調達時の情報セキュリティ要件の明確化に係る説明の追加等の見直しを行った。

（ア）オンライン研修（ｅ－ラーニング）

省内ＬＡＮシステムの自習室機能を利用したオンライン研修を行っており、職員は、１年中いつでも都合のよい時に情報セキュリティ研修を受講できる。受講コースは、全職員向けの基礎コースと各責任者・管理者向け専門コースの２つを用意しており、対象者の役割に応じて受講する。またテスト機能により、自らの理解度を確認することが可能である。

なお、オンライン研修の受講状況は、四半期ごとに各部局等へ報告しており、未受講者に対する受講督促に供している。

（イ）オフライン研修

自習室機能を利用できない職員（一部地方支分部局、施設等機関等）に対して、統括情報セキュリティ責任者から該当部局等へ、オンライン研修と同等の内容の電子媒体教材（ＣＤ－Ｒ）を配布し、情報セキュリティ研修の実施に供している。

（ウ）集合研修

異動者の多い時期（４月及び１０月）を考慮し、新規採用職員・他省庁等からの転入職員に対してセキュリティポリシー全般に係る集合研修を行った。

１０月には、全職員向けのセキュリティポリシーの基礎研修及び各情報システムの責任者・管理者等向けの専門研修を実施する等、対象者の役割に応じた集合研修を行った。

これらの研修は、セキュリティポリシー及び関連規程類の理解はもとより、最新の障害・事故等の事例解説や、受講者自らが操作する内容を盛り込むことで、より実践を意識したものとしている。

（エ）訓練

標的型メール攻撃に用いられるメールは、業務メールを装って送信される

ため真偽の判断が困難であるとともに、特定の個人や組織のみが対象とされるためウイルス情報が出回りづらく、ウイルス対策ベンターにおける対応が遅くなる傾向がある。

このような状況を踏まえ、標的型メール攻撃に対する対処方法や見分け方等の教育を行うとともに、NISC との連携のもと、標的型メールを模したメールを実際に職員に送付し、標的型メールを初めとした不審メールの受信時における対応を確認するための訓練を、教育の一環として実施した。

また、訓練結果について、CISO からの講評及びメッセージを添えて職員へ報告することにより、標的型メール攻撃に対する意識の向上を図った。

（オ）その他

政府機関の情報システムにおいては、情報セキュリティ対策を適切に講じるため、企画・設計段階から情報セキュリティ対策を考慮し、必要な情報セキュリティ要件を適切に調達仕様に組み込むことが求められる。

このような状況を踏まえ、NISC より公開された「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」（以下「ＳＢＤ（※）マニュアル」という。）の活用を促進するための研修を、NISC との連携のもと、教育の一環として実施した。

（※）Security By Design の略称。情報システムを企画・設計段階から確保するための方策のこと。

③　普及・啓発

電子政府利用促進週間や情報セキュリティ月間、人事異動者の多い時期、障害・事故等の発生時といった情報セキュリティに関連するイベントや、情報システムに係わる職員が集まる会議の機会等をとらえ、セキュリティポリシー及び関連規程類の職員への周知を行うことにより、一層の理解促進を図った。

（３）情報セキュリティ対策実施状況の自己点検

①　概要

情報セキュリティ対策実施状況の自己点検（以下「自己点検」という。）は、省内全職員を対象に、セキュリティポリシーに基づく各自の役割に応じた情報セキュリティ対策の実施状況を自ら点検することで、自己の情報セキュリティ対策の実効性を確保・向上させるために毎年度行っており、把握率・実施率・到達率（表１）の３つの評価基準により評価している。

なお、自己点検の実施に当たっては、年度ごとに、方針、対象、点検内容、実施時期、評価方法等を記した「情報セキュリティ対策の実施状況に係る自己点検計画」を策定し、適切な自己点検の実施を図っている。

また、平成 23 年度においては、従来の自己点検が網羅性を重視していたため、点検項目のボリュームが大きくメリハリがなく、その結果、重要な事項が身についていないなど実施が形骸化しているのではないかとの反省から、点検項目を重点化するとともに、事前のチェックリストの配布やケーススタディの導入により、情報セキュリティ対策に関する意識と理解度の向上を図ることとした。

表１　自己点検の評価基準

評価基準	基準の内容
把握率	対策実施状況が把握できた者の割合
実施率	把握した者のうち、責務が生じた者に占める対策を実施した者の割合
到達率	把握した者のうち、責務が生じた一定の割合（100%, 95%, 90%）以上の者が対策を実施した遵守事項の割合

なお、平成 22 年度の点検結果は、対策は概ね適切に実施されていたが、行政事務従事者及び情報システム責任者・管理者の到達率に不十分な点が見受けられるため、対策をすみずみまで浸透させることが必要というものであった。

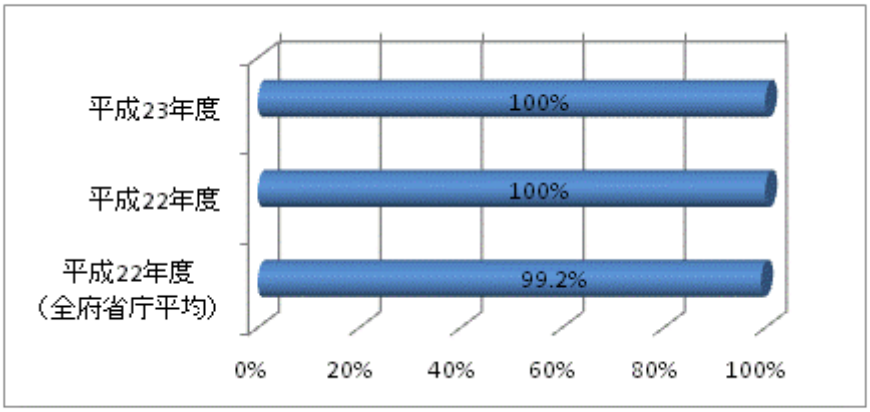
これを受け、平成 23 年度においては、セキュリティポリシーの理解促進のため、研修教材を見直すとともに、部局ごとのオンライン研修の受講状況を四半期ごとに周知することにより、職員への研修受講の意識付けを行った。また、役割に応じた重点項目のチェックリストを作成・配布する等により、対策の浸透を図った。

② 結果の状況

（ア）把握率

図２のとおり、平成 22 年度に引き続き把握率 100%を達成した。

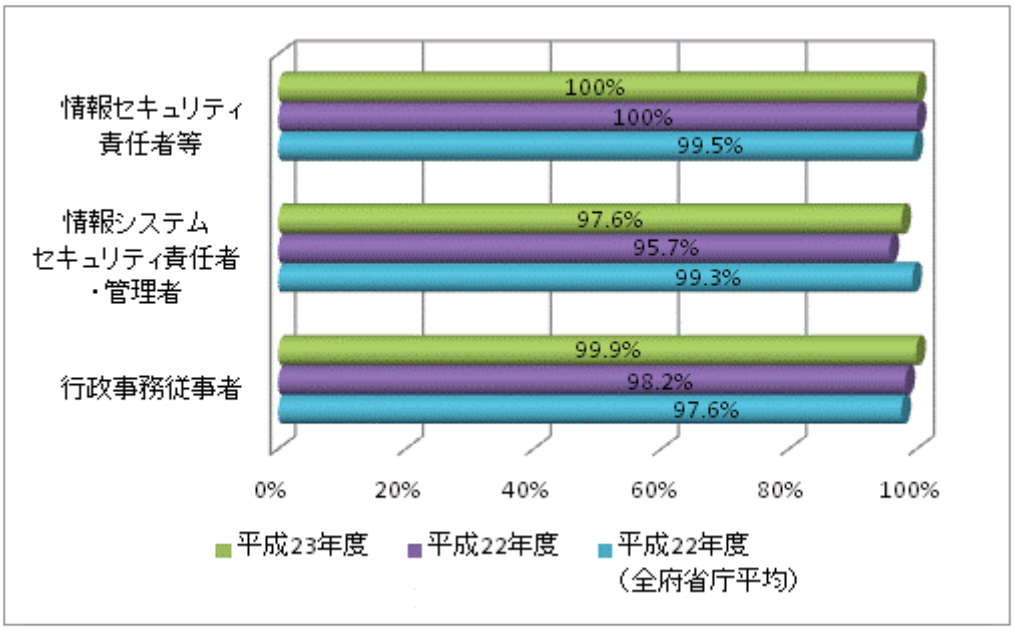
図２　把握率



（イ）実施率

図３のとおり、情報セキュリティ責任者等は、平成 22 年度に引き続き実施率 100%を達成した。情報システムセキュリティ責任者・管理者は 97.6%、行政事務従事者は 99.9%と、いずれも増加となった。

図３　主体別の実施率



（ウ）到達率

情報セキュリティ責任者等は、全対象者が対策を実施したことで、到達率 100%を達成した（図４－１）。情報システムセキュリティ責任者・管理者は、

到達率 100%は減少（20.8%）、95%以上は増加（83.3%）、90%以上も増加(95.8%)となった（図４－２）。行政事務従事者は、到達率 100%は減少（0%）、95%以上は増加（100%）、90%以上も増加（100%）となった（図４－３）。

図４－１　主体別の到達率（情報セキュリティ責任者等）

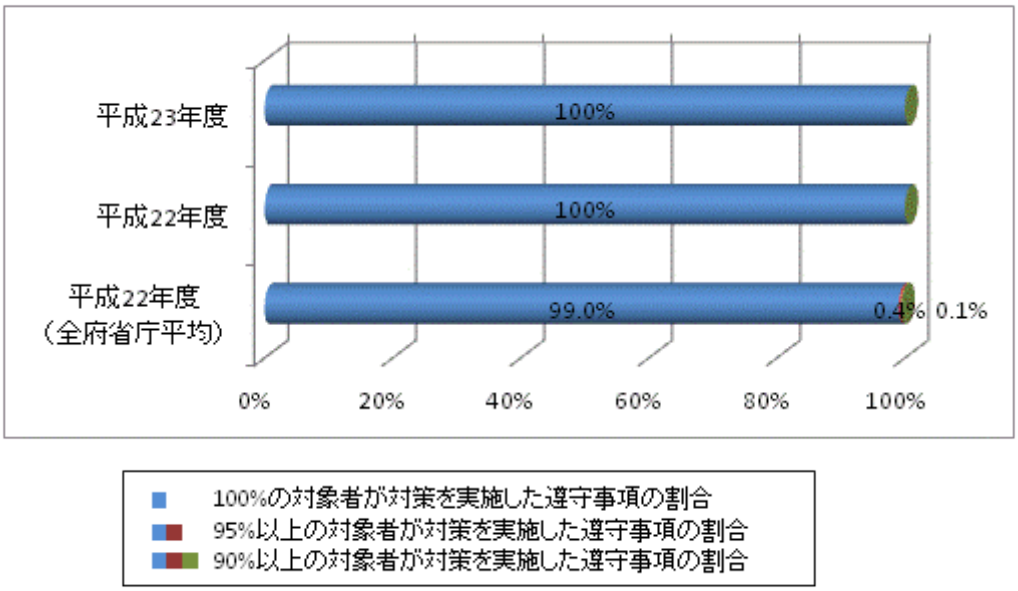


図４－２　主体別の到達率（情報システムセキュリティ責任者・管理者）

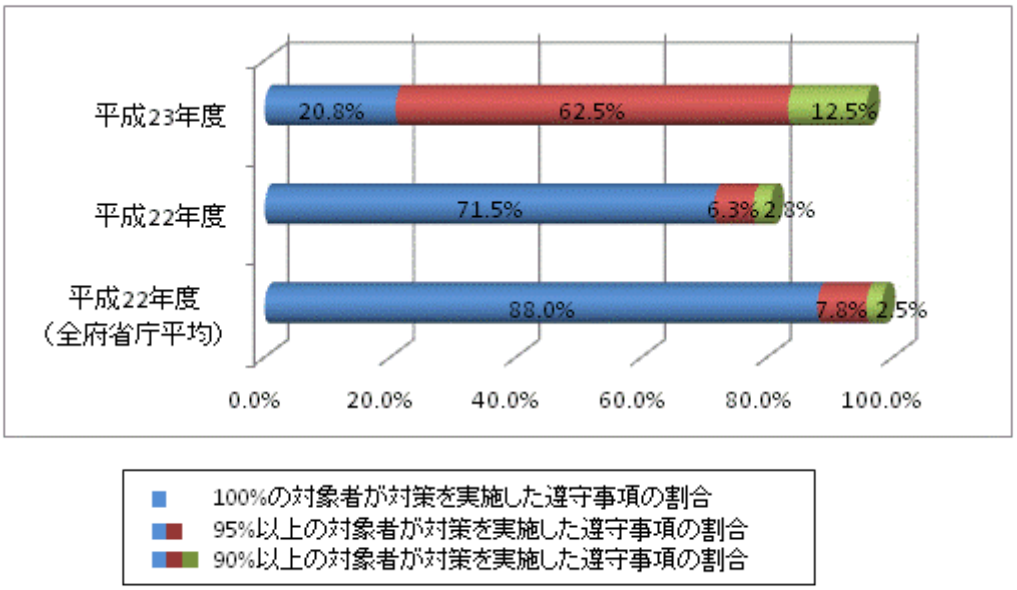
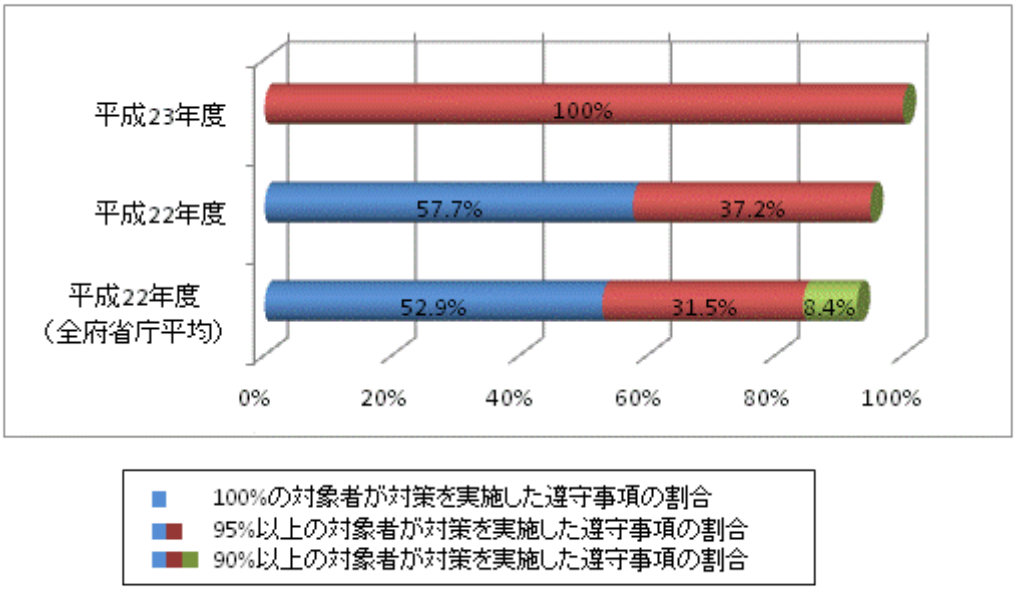


図４－３　主体別の到達率（行政事務従事者）



③　総括

概要で述べたとおり、従来の網羅的な点検方法を改め、点検項目を重点化したことにより、平成 22 年度の結果との単純比較はできないが、全体的に実施率が向上したこと、到達率（95%及び 90%）が向上したことから、必要な対策については概ね適切に実施されたことがわかる。

しかし、情報システムセキュリティ責任者・管理者については、到達率（100%及び 95%）が平成 22 年度より向上したものの、全府省庁平均を下回った。この主な原因としては、セキュリティポリシー及び関連規程類の理解不足が考えられるが、特に、これまで情報システムの管理・運用等に携わってこなかった職員が異動に伴い担当となる場合において、これまでは自らが対策実施主体ではなかった遵守事項に対する遵守意識が希薄であることが、理解不足を招いているものと思われる。

このため、これらの役割にある職員に対し、適切な時期を踏まえ、割り当てられた役割の確認を促す必要があるとともに、セキュリティポリシー及び関連規程類の周知・徹底や、研修内容及び教材の見直し等による情報セキュリティ教育の充実を図る必要がある。

（４）情報システムの重点検査

①　概要

情報システムの重点検査は、厚生労働省で導入している情報システムごとの公開ウェブサーバ・電子メールサーバを対象に、セキュリティポリシーに準拠した情報セキュリティ対策が実施されているかを確認するために毎年度行っており、表２のとおり実施率に基づく評価基準により評価（Ａ～Ｄ）している。

平成 23 年度においては、従来からの調査内容の継続性にこだわらず、必要な調査項目の精査・深掘りを行い、より実効性を高める検査とした。

表２　重点検査の評価基準

評 価	実 施 率
A	X = 100 %
B	80 % ≦ X ＜ 100 %
C	60 % ≦ X ＜ 80%
D	X ＜ 60 %

なお、平成 22 年度の検査結果（不正プログラム対策・不正アクセス対策・サーバ管理に関する状況を検査）は、公開ウェブサーバ・電子メールサーバとも「A」評価であった。

② 結果の状況

（ア）公開ウェブサーバ

すべての公開ウェブサーバにおいて、検査項目（表３）に対する対策実施状況の評価は「A」評価であった。

表３　公開ウェブサーバに対する重点検査項目

対策内容	重点検査項目
ウェブサーバに関する脆弱性の調査	平成22年度に複数省庁で検出された脆弱性の調査 ・SSL バージョン 2 の無効化状況 ・SSL 通信で弱い暗号方式の無効化状況
昨今のセキュリティトピックへの対策の調査	大量パケット送信型の DoS(Denial of Service attack（注)) 攻撃のための対策状況 ・電子計算機及び通信回線装置が装備している機能を使用した DoS 攻撃への対応状況 ・DoS 攻撃を受けた場合、影響最小化への対応状況 ・Dos 攻撃に関する監視対象の特定と、監視方法及び監視記録の保存期間策定への対応状況 ・DoS 攻撃発生時の対処手順や連絡体制整備の対応

	状況
対策実施状況との関係の調査	・0S 及びサーバアプリケーションのセキュリティアップデート状況の調査

（注）サーバ等のネットワーク構成機器に対する攻撃により、サービスの提供を不能な状態にすること。

（イ）電子メールサーバ

すべての電子メールサーバにおいて、検査項目（表４）に対する対策実施状況の評価は「A」評価であった。

表４　電子メールサーバに関する重点検査項目

対策内容	重点検査項目
対策実施状況との関係の調査	・0S 及びサーバアプリケーションのセキュリティアップデート状況の調査

③　総括

平成 23 年度の検査の結果は、すべての検査において「A」評価（実施率 100%）であった。今後も引き続き、この状態を維持できるよう適切な情報セキュリティ対策の実施に努めていく。

（5）情報セキュリティ監査

①　概要

情報セキュリティ対策の実施体制の構築及び対策の実施に関する全般的な状況の確認を目的として、情報セキュリティ監査を毎年度行っている。実施結果については、指摘事項の内容により、即時的に省内に注意喚起する等の対応を行っているほか、翌年度以降の情報セキュリティ対策の改善と実効性の向上のために活用している。

監査の実施に当たっては、年度ごとに、方針、対象、方法、判断基準等を記した「厚生労働省情報セキュリティ監査計画書」を策定し、適切な監査の実施を図るとともに、客観性・独立性を確保し、専門性の高い監査とするため、外部の専門家を活用している。

②　内容

（ア）関係規程に関する準拠性監査

ｉ　統一基準群とセキュリティポリシーの準拠性の監査

セキュリティポリシーが統一基準群に準拠しているかを確認する監査。

ii　セキュリティポリシーと関連規程類の準拠性の監査

省統一の関連規程類がセキュリティポリシーに準拠しているかを確認する監査。今回の監査対象の関連規程類は、平成 23 年度に改訂を行った９文書のうち、形式的な修正のみであった文書を除く、以下の７文書である。

○　情報取扱手順書
○　情報セキュリティ対策実施手順書作成のガイドライン
○　障害・事故等対処手順書
○　人事異動等の際に行うべき情報セキュリティ対策実施規程
○　厚生労働省支給以外の情報システムによる情報処理の手順書
○　省外でのＰＣの利用における情報処理の手順書
○　外部委託における情報セキュリティ対策実施手順書

iii　セキュリティポリシーと各情報システムの情報セキュリティ対策実施手順書の準拠性の監査

厚生労働省が運用する情報システムから、情報システムのライフサイクル等を考慮して選定した６システムについて、各情報システムの情報セキュリティ対策実施手順書がセキュリティポリシーに準拠しているかを確認する監査。

（イ）自己点検に関する監査

i　情報セキュリティ管理体制に関する監査

組織全体の傾向が把握できるサンプル数の自己点検票を用いて、セキュリティポリシーに基づく対策実施主体別の情報セキュリティ対策の実施状況を確認する監査。対策実施主体は、以下のとおり。

○　統括情報セキュリティ責任者
○　情報セキュリティ責任者
○　課室情報セキュリティ責任者
○　情報システムセキュリティ責任者
○　情報システムセキュリティ管理者

ii　情報システムに対する情報セキュリティ対策の実施状況に関する監査

②（ア）iiiの６システムについて、セキュリティポリシー及び自己点検結果等をもとに、各情報システムの運用担当者及び利用者を対象にヒアリング

を行い、各情報システムの情報セキュリティ対策実施手順書が適正に運用されているかを確認する監査。

iii　執務室における情報セキュリティ対策の実施状況に関する監査

組織全体の傾向が把握できるサンプル数の自己点検票を用いて、セキュリティポリシーに基づく行政事務従事者の情報セキュリティ対策の実施状況を確認する監査。

（ウ）その他の監査

ⅰ　平成 22 年度に実施した監査で指摘された課題及び問題点に対する改善状況の監査

平成 22 年度に実施した監査において指摘された事項について、改善状況を確認する監査。

ii　例外措置の申請及び許可状況の監査

例外措置の申請及び許可が、セキュリティポリシー及び例外措置手順書に基づき適正に行われているかを確認する監査。

③　総括

（ア）関係規程に関する準拠性監査

ⅰ　統一基準群とセキュリティポリシーの準拠性の監査

監査対象のセキュリティポリシーについては、概ね統一基準群に準拠していることが確認された。

ii　セキュリティポリシーと関連規程類の準拠性の監査

監査対象の 7 文書については、概ねセキュリティポリシーに準拠していることが確認された。

iii　セキュリティポリシーと各情報システムの情報セキュリティ対策実施手順書の準拠性の監査

監査対象の情報セキュリティ対策実施手順書については、一部に規定すべき事項の不備または不足が発見されたため、直ちに修正を指示したが、その他の情報セキュリティ対策実施手順書については、概ねセキュリティポリシーに準拠していることが確認された。

（イ）自己点検に関する監査

ⅰ　情報セキュリティ管理体制に関する監査

監査対象の対策実施主体が行うべき情報セキュリティ対策については、概ねセキュリティポリシーが適切に遵守され、実施されていることが確認された。

ⅱ　情報システムに対する情報セキュリティ対策の実施状況に関する監査

監査対象のすべての情報システムにおいて、情報セキュリティ対策の多くが適切に実施されていることが確認された。しかしながら、直ちに情報セキュリティ事案を引き起こすものではないが、監査対象の情報システム全般において、外部委託先の管理に関し改善すべき点があるとの指摘がなされた。

これを受け、監査対象のすべての情報システムの運用担当者に対する改善の指示のほか、すべての情報システムの運用担当者に対する注意喚起を実施した。

ⅲ　執務室における情報セキュリティ対策の実施状況に関する監査

監査対象の行政事務従事者が行うべき情報セキュリティ対策については、概ねセキュリティポリシーが適切に遵守され、実施されていることが確認された。しかしながら、一部の情報システムにおいて、情報セキュリティ対策の教育や情報の取扱いに関し改善すべき点があるとの指摘がなされた。

これを受け、当該情報システムの運用担当者に対する改善の指示を実施した。

（ウ）その他の監査

ⅰ　平成 22 年度に実施した監査で指摘された課題及び問題点に対する改善状況の監査

指摘された課題及び問題点については、すべて対応が完了した。

ⅱ　例外措置の申請及び許可状況の監査

例外措置の申請はなかった。

（６）調達・外部委託

情報処理業務を外部に委託する際には、委託先においてもセキュリティポリシーと同等の対策を実施する必要がある。このため、外部委託を行う業務の範囲や外部委託の実施に係る検討手順、調達仕様書への記載要件の検討事項等を「外部委託における情報セキュリティ対策実施手順書」としてまとめ、調達担当者がこれを遵守することにより、外部委託による業務の遂行に必要な情報セキュリティ

水準の確保を図っている。手順書においては、調達仕様書への記載例も示しており、調達担当者はこれをカスタマイズして記載することが可能であるとともに、これにより記載事項の標準化を図っている。

また、外部委託の実施に際し必要となる情報セキュリティ要件を、企画・設計段階から検討し、その結果を適切に調達仕様書に反映することが重要である。このため、企画・設計段階において調達仕様書に記載すべき情報セキュリティ要件の策定を支援するＳＢＤマニュアルの普及を図るとともに、この活用方法を習得するための研修を実施し、これにより適切な情報セキュリティの確保を図っている。

なお、調達仕様書については、その作成過程において、ＣＩＯ補佐官を中心に、ＰMO（プログラム・マネジメント・オフィス）による審査が実施され、その中で情報セキュリティ要件も確認されている。

（７）障害・事故等に対する取組

①　概要

情報セキュリティに関する障害・事故等への適切な対処を行うことを目的として、障害・事故等が発生した場合等の対処及び報告等の手続を規定した「障害・事故等対処手順書」を整備しており、これに基づき、障害・事故等における影響の拡大防止と迅速な復旧を図っている。

また、NISC との連携のもと、サイバー攻撃発生に備えた訓練を実施し、対処手順を確認した。

②　障害・事故等の概要

情報セキュリティに関する障害・事故等については、以下の発生を確認した。

（ア）労働基準行政情報システム・労災行政情報管理システムのウイルス感染

＜発見日＞

平成 23 年 11 月 25 日　午前 11 時ころ

＜概要＞

労働基準行政情報システム・労災行政情報管理システムの端末において、業務情報を得るため特定のホームページへアクセスした際に、不正な動きをするプログラムが自動的にダウンロード（ショートカットの作成）され、このショートカットをクリックしたところウイルスに感染したもの。

感染確認後、システム全体におけるインターネット接続の遮断や当該ウイルスの削除、当該ウイルスの新たな侵入に備えたシステム設定の変更等の対

応を速やかに行うとともに、ウイルス対策ベンダーに検体を提供し、即日公開された免疫プログラムを適用の上、システム内に当該ウイルスが存在しないことを確認した。なお、事案に伴う両システムへの影響及び情報漏えい等は確認されていない。

再発防止策としては、両システムの利用者に対し、不審なファイルの実行（クリック）禁止等の確実に実行することが重要な措置や不審なファイル等を確認した場合の対応について周知・徹底を図るとともに、省内の職員に対する技術的な情報の提供も含めた注意喚起を実施した。

（イ）愛知労働局におけるＵＳＢメモリの紛失

＜発見日＞

平成 23 年 12 月 17 日　午前 0 時ころ

＜概要＞

愛知労働局管内の名古屋東労働基準監督において、業務上保有している個人情報を保存したＵＳＢメモリを鞄に入れて庁舎外へ持ち出し、鞄ごと紛失したもの。

個人情報が漏えいした可能性があることから、関係者に謝罪するとともに、ＵＳＢメモリの管理状況についての緊急点検を実施し、その結果を踏まえた再発防止策として、外部電磁的記録媒体の使用について、業務上の必要性から全面使用禁止は難しいものの、情報システムにおいて一定の制限をかけることとした。また、同局を含む省内の職員に対する注意喚起を実施した。

（ウ）関東信越厚生局におけるＵＳＢメモリの紛失

＜発見日＞

平成 24 年 2 月 9 日　午前 9 時ころ

＜概要＞

関東信越厚生局麻薬取締部横浜分室において、拘置所における被疑者の取り調べを終え、貸与された生体認証付ＵＳＢメモリに、当該被疑者の供述等の捜査情報を上書きし、取調用鞄に戻した後、公用車で職場に戻り、取調用鞄を職場に置いて帰宅した。翌日、引き続き取り調べを実施するため、職場で取調用鞄を開けたところ、紛失が判明したもの。

再発防止策としては、捜査情報が入った電磁的記録媒体の取扱いについて万全を期し、同様の事案を発生させないよう管理の徹底を図った。また、同局を含む省内の職員に対する注意喚起を実施した。

（エ）国立感染症研究所ホームページへの不正アクセス

＜発見日＞

平成 24 年 3 月 25 日　午後 16 時ころ

＜概要＞

国立感染症研究所において、ウェブサーバが侵入者により不正にアクセスされ、コンテンツが改ざんされたもの。不正アクセスの確認後、サーバ機器の交換（旧サイト）等の対策を講じた。なお、データベースサーバへの侵入及び保有する個人情報等のデータの漏えいは認められていない。

再発防止策としては、各部局の情報システムにおけるセキュリティ確保について、同研究所を含む担当職員に対する注意喚起を実施した。また、原因を究明の上、不正アクセスを防止するための対策を検討中である。

③　訓練の概要

NISC との連携のもと、標的型メールを模したメールを実際に職員に送付し、標的型メールを初めとした不審メールの受信時における対応を確認するための教育訓練を実施したほか、政府機関情報セキュリティ横断監視・即応調整チーム（NISC 内に整備された、政府横断的な情報収集、攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有を行うための体制（Government Security Operation Coordination Team。以下「GSOC」という。））との間で、サイバー攻撃発生時における対応及び連絡体制を確認するための訓練を実施した。

④　その他

その他の取組としては、ゴールデンウィーク、夏季休暇集中期及び年末年始の前や省内外の情報セキュリティ事案発生時等の機会をとらえ、緊急時連絡体制の再確認を行ったほか、最新の情報セキュリティを取り巻く状況を踏まえ、障害・事故等対処手順書を改訂した。

（８）　その他の取組事項

①　職員に対する周知等

（ア）情報セキュリティ事案に関する注意喚起

NISC（GSOC）から提供される情報セキュリティ事案に関する情報については、即時的に省内へ注意喚起している。また、省内で情報セキュリティ事案の発生・予告を確認した場合には、速やかに省内へ注意喚起するとともに、NISC（GSOC）へ報告している。

（イ）不審メール等に関する注意喚起

GSOC から提供される不審メール情報、脆弱性情報、修正パッチの公開情報等については、即時的に省内へ注意喚起している。また、職員宛てに不審メールが送付された場合も、速やかに省内へ注意喚起するとともに、GSOC へ報告している。

（ウ）イントラネットにおける情報提供

セキュリティポリシー及び関連規程類や各種研修教材、不審メール情報、脆弱性情報等の情報セキュリティ対策に関連する情報については、日常的に参照できるよう、常に最新の情報を省内ＬＡＮシステム上に掲載している。

（エ）最高情報セキュリティアドバイザーによる講義

集合研修に際し、最高情報セキュリティアドバイザーによる講義の時間を設け、情報セキュリティに関する講義を行った。

② 外部研修・勉強会等の活用

情報セキュリティ対策の推進のためには、対策実施担当者の情報セキュリティ対策に係る知識の向上も重要である。このため、総務省が主催する情報システム統一研修を受講したほか、NISC が主催する情報セキュリティ勉強会に参加した。

③ 公開ウェブサーバ脆弱性検査

厚生労働省で実施する情報セキュリティ監査とは別に、政府機関情報システムの情報セキュリティ対策の向上のため、NISC の主催による公開ウェブサーバに対する脆弱性検査が実施された。厚生労働省においても１つの情報システムが検査を受けた結果、一部に脆弱性が確認されたが、当該脆弱性への対応は既に完了した。

④ 推奨事例への対応

NISC は、平成 22 年度に各府省庁が実施した情報セキュリティ対策の中から、いくつかの取組を推奨事例として選定した。平成 23 年度に実施した対策のうち、標的型メール攻撃に対する教育訓練及び自己点検内容の重点化については、推奨事例として選定されたことも踏まえ、実施の必要性や方法を検討し、新たな取組として実施した。

3　情報セキュリティ対策に関する平成 24 年度の計画

平成 24 年度における情報セキュリティ対策は、平成 23 年度に実施した対策を引き続き着実に実施することを基本とするが、全体的な実施効果の底上のため、各対策において改善に向けた検討を行い、内容の一層の充実を図ることとする。

特に、サイバー攻撃や情報漏えいといった情報セキュリティ事案に係る以下の対策については、最新の状況を十分に考慮しながら、重点的に取り組んでいく。

（1）情報セキュリティ教育の充実

情報セキュリティ教育を通じ、障害・事故等への対処や情報の適切な取扱いについて周知・徹底する。教育教材や内容についても、理解しやすいものとなるよう見直す。

また、サイバー攻撃については、最新の状況を踏まえた教育を実施し、対策の重要性について意識の向上を図る。

（2）障害・事故等に備えた連絡体制の構築・確認

サイバー攻撃を始めとする障害・事故等の迅速かつ適切な報告及び対処を可能とするため、情報システムの管理・運用等を行う職員に対し、常日頃からの連絡体制及び対処手順の確認を呼びかける。

また、サイバー攻撃については、省内関係部局との連絡体制を見直すとともに、NISC との連携を密に行い、事案の予告や発生に備える。

終わりに　～最高情報セキュリティアドバイザーからのメッセージ～

厚生労働省の施策は、国民生活と密接に関連した、年金、医療、育児、介護、雇用等を扱い、関連する情報資産には様々な個人情報を含む上に、情報システムも多岐にわたります。この情報システムの中には、社会保険オンラインシステムやハローワークシステムのような全国の地方支分部局、施設等機関にまたがる大規模システムも含まれていて、一旦、インシデントが発生すると国民生活にも影響を与えかねません。このため、厚生労働省においてもセキュリティポリシー等を遵守し、着実に PDCA を実践し、課題があれば一層の改善を行っていくことが重要になります。

公開ウェブサーバ、電子メールサーバの重点検査については、前年度に引き続き「A評価」であり、一定の成果を収めているものの、情報セキュリティ対策実施状況の自己点検結果においては、改善はみられたものの、情報システムセキュリティ責任者・管理者の到達率において、全府省平均に達していません。このため、情報セキュリティ教育やシステム監査等において、一層の情報セキュリティ対策への助言と支援を行う所存です。

また、平成 23 年度は、NISC と連携し、事業継続計画（情報システム運用継続計画）の策定、標的型メール訓練の実施、省内職員向けの SBD 研修の実施など更なるセキュリティ向上に向けた新たな試みを開始した事は評価できると思われます。
特に、昨年の東日本大震災での経験を踏まえ、個別システムの事業継続計画（情報システム運用継続計画）を策定の緒に就いた事は評価できます。まだ未整備の個別システムも多く存在するため、その策定を推進することが重要であると考えます。

一方セキュリティに関する事故・障害が数件発生いたしました。その中には、セキュリティポリシーが遵守されれば防止できた案件も含まれています。地方支分部局や施設等機関での発生が多いため、これらへの情報セキュリティ研修の充実が必要と考えられます。

今後は概算要求確認時、調達仕様書審査時、提案書審査時等の様々な局面において、情報セキュリティ要件および業務継続性要件について重点課題として確認、助言を行っていく所存です。

最高情報セキュリティアドバイザー
（厚生労働省ＣＩＯ補佐官）
徳永　篤男